Tadeusz Pezda

On some issues concerning polynomial cycles

Communications in Mathematics, Vol. 21 (2013), No. 2, 129--135

Persistent URL: `http://dml.cz/dmlcz/143586`

Communications in Mathematics 21 (2013) 129–135

On some issues concerning polynomial cycles

Tadeusz Pezda

Abstract. We consider two issues concerning polynomial cycles. Namely, for a discrete valuation domain R of positive characteristic (for $N \geq 1$) or for any Dedekind domain R of positive characteristic (but only for $N \geq 2$), we give a closed formula for a set $\mathcal{CYCL}(R, N)$ of all possible cycle-lengths for polynomial mappings in R^N. Then we give a new property of sets $\mathcal{CYCL}(R, 1)$, which refutes a kind of conjecture posed by W. Narkiewicz.

1 Introduction

For a commutative ring R with unity and $\Phi = (\Phi_1, \dots, \Phi_N)$, where $\Phi_i \in R[X_1, \dots, X_N]$, we define a *cycle* for Φ as a k-tuple $\bar{x}_0, \bar{x}_1, \dots, \bar{x}_{k-1}$ of different elements of R^N such that

$$\Phi(\bar{x}_0) = \bar{x}_1,\ \Phi(\bar{x}_1) = \bar{x}_2\,,\ \dots\ ,\ \Phi(\bar{x}_{k-1}) = \bar{x}_0\,.$$

The number k is called the *length* of this cycle.

Let $\mathcal{CYCL}(R, N)$ be the set of all possible cycle-lengths for polynomial mappings in N variables with coefficients from R (we clearly assume that the elements of the considered cycles lie in R^N). For a material on various aspects of polynomial mappings and arithmetic of dynamical systems, see [1] and [4].

In Section 2 we examine $\mathcal{CYCL}(R, N)$ for a discrete valuation domain R with maximal ideal P. We assume that the residue field R/P has p^f elements (if R/P is infinite, then $\mathcal{CYCL}(R, N) = \mathbf{N}$). It is known (see Fact 1 in Section 2) that any element $k \in \mathcal{CYCL}(R, N)$ is of the form $k = a \cdot p^\alpha$, where all possible a were completely determined by the author. Thus, in order to know $\mathcal{CYCL}(R, N)$ it suffices for a given 'possible' a (as explained before) to find all α such that $a \cdot p^\alpha \in \mathcal{CYCL}(R, N)$. It is known that for a finite ramification index e the numbers α are bounded from above by some explicit function depending on e, p, f, N. In Theorem 1 we give a bound from below (for a given 'possible' a) for the biggest α

2010 MSC: 11R09, 13F05, 37P35
Key words: polynomial cycles, discrete valuation domains, Dedekind rings

such that $a \cdot p^{\alpha} \in \mathcal{CYCL}(R, N)$. Namely, we receive

$$\alpha \geq \left\lfloor \log_p \left(\frac{\log_p e}{2fN} \right) \right\rfloor .$$

We see that for fixed f, p, N the right-hand side of the last inequality grows to ∞ (when $e \to \infty$). Note that for a discrete valuation domain R the set $\mathcal{CYCL}(R, N)$ does not depend solely on p, e, f, N. Sometimes some subtler properties of R should be taken into account.

As a consequence of Theorem 1, in Theorem 2 we determine the sets $\mathcal{CYCL}(S, N)$ for some Dedekind domains S of positive characteristic and some N.

In Section 3 we consider properties of $\mathcal{A} := \mathcal{CYCL}(R, 1)$ for a domain R. Any such $\mathcal{A}$ satisfies the following three 'obvious' properties:

(i) $1, 2 \in \mathcal{A}$;

(ii) $\mathcal{A}$ is closed under taking divisors;

(iii) for any prime p from $p \in \mathcal{A}$ it follows that $[1, p] \subseteq \mathcal{A}$.

Since there were no other obvious properties of $\mathcal{A}$, in mid-nineties W. Narkiewicz conjectured that for $\mathcal{A} \subseteq \mathbf{N}$ satisfying (i), (ii), (iii) there exists a domain R such that $\mathcal{A} = \mathcal{CYCL}(R, 1)$. In Section 3 we give a negative answer to this question.

I think that it would be interesting to give a sensible conjecture concerning sets $\mathcal{CYCL}(R, N)$ for $N \geq 2$. In particular it is not clear whether the above property (iii) holds in this case.

2 Finding $\mathcal{CYCL}(R, N)$ for some rings of positive characteristic

Let R be a discrete valuation domain of any characteristic, and P is the unique maximal ideal of R. We assume that the field R/P is finite and has p^f elements (for prime p). Let π be a generator of the principal ideal P, and let v be the norm of R, normalized so that $v(\pi) = 1/p$. We denote by w the corresponding exponent, defined by

$$w(x) = -\frac{\log v(x)}{\log p} \quad \text{for } x \neq 0\,, \quad \text{and} \quad w(0) = \infty\,.$$

We put $e := w(p)$. Thus e is the ramification index of R. We extend w to R^N by putting $w(x_1, \ldots, x_N) = \min\{w(x_1), \ldots, w(x_N)\}$.

A polynomial cycle $\bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{k-1}$ is called a *(polynomial) $\star$-cycle* if

$$w(\bar{x}_i - \bar{x}_j) \geq 1 \quad \text{for all } i, j\,.$$

Let $\mathcal{CYCL}\star(R, N)$ be the set of all possible lengths of $\star$-cycles for polynomial mappings in N variables with coefficients from R.

In the fact below we collect some properties of $\mathcal{CYCL}(R, N)$ already proved by the author (see [2], [3]).

Fact 1. *Let $R, p, f, \ldots$ be as above. Then*

(i) a number k lies in $\mathcal{CYCL}(R, N)$ if and only if $k = ab$, where $a \leq p^{fN}$ and b is the length of a suitable $\star$-cycle in R^N.

(ii) If $\widehat{R}$ is the completion of R with respect to the norm v, then

$$\mathcal{CYCL}(R,N) = \mathcal{CYCL}(\widehat{R},N) \quad \text{and} \quad \mathcal{CYCL}\star(R,N) = \mathcal{CYCL}\star(\widehat{R},N)$$

(note that for $\widehat{R}$ the numbers p, e, f are the same as for R).

(iii) Let m be a positive integer not divisible by p. Then there is a $\star$-cycle of length m in R^N if and only if there are $r > 0$ and positive integers $a_1, \dots, a_r$ with $a_1 + \cdots + a_r \le N$ such that m divides $[p^{fa_1} - 1, \dots, p^{fa_r} - 1]$.

(iv) Let S be a Dedekind domain, and let $\mathcal{P}(S)$ denote the family of all nonzero prime ideals of S. If $N \ge 2$, then

$$\mathcal{CYCL}(S,N) = \bigcap_{\mathfrak{p}\in\mathcal{P}(S)} \mathcal{CYCL}(S_{\mathfrak{p}},N) = \bigcap_{\mathfrak{p}\in\mathcal{P}(S)} \mathcal{CYCL}(\widehat{S_{\mathfrak{p}}},N),$$

where $\widehat{S_{\mathfrak{p}}}$ is the completion of $S_{\mathfrak{p}}$ with respect to the obvious valuation.

In particular, to find $\mathcal{CYCL}(R,N)$ it suffices to know p^f and, for each m dividing $[p^{fa_1} - 1, \dots, p^{fa_r} - 1]$ (for some $a_1, \dots, a_r$ satisfying $a_1 + \cdots + a_r \le N$), to know for which $n \ge 0$ the number $m \cdot p^n$ lies in $\mathcal{CYCL}\star(R,N)$.

In this section we will prove that for any 'possible' m, as explained in Fact 1(iii), and for any n if the ramification index is sufficiently large, then $m \cdot p^n \in \mathcal{CYCL}\star(R,N)$. This, in turn, gives a closed formula for $\mathcal{CYCL}(S,N)$ for a Dedekind domain S of positive characteristic and $N \ge 2$. The fact that for any prime p and any $n \ge 0$ in $F_p[[X]]$ there are cycles of length p^n was established in the thesis of Zieve [5], who quoted an example due to Poonen.

Theorem 1. *Let R be as in this section. Let m be a divisor of $[p^{fa_1} - 1, \dots, p^{fa_r} - 1]$ for some $a_1, \dots, a_r$ satisfying $a_1 + \cdots + a_r \le N$. If $e \ge p^{2fNp^n}$, then $m \cdot p^n \in \mathcal{CYCL}\star(R,N)$.*

Proof. Owing to Fact 1, we may assume that $n \ge 1$ and R is complete. It suffices to take $m = [p^{fa_1} - 1, \dots, p^{fa_r} - 1]$. Suppose that for $e \ge p^{2fNp^n}$ we have a $\star$-cycle of length $(p^{fa_1} - 1) \cdot p^n$ for a map $\Phi_1 \colon R^{a_1} \to R^{a_1}$. For $i \ge 2$, by Fact 1(iii), in R^{a_i} there is a $\star$-cycle of length $p^{fa_i} - 1$ for some mapping Φ_i of R^{a_i}. We see that $\Phi = (\Phi_1, \dots, \Phi_r) \colon R^{a_1+\cdots+a_r} \longrightarrow R^{a_1+\cdots+a_r}$ constructed in the natural way has a $\star$-cycle of length $[(p^{fa_1} - 1) \cdot p^n, p^{fa_2} - 1, \dots, p^{fa_r} - 1] = m \cdot p^n$.

So, it suffices to prove for any $M \le N$ that $(p^{fM} - 1) \cdot p^n \in \mathcal{CYCL}\star(R,M)$.

Put $q = p^{fM}$, and let ξ be a primitive root of unity of order $q - 1$. By the usual Hensel's lemma (here we use the completeness of R) we have that the minimal over R polynomial of ξ is of degree M. Thus $R^M \sim R[\xi]$ as modules over R. Using this canonical isomorphism, we obtain that to any polynomial $F(X) \in R[\xi][X]$ there corresponds a polynomial mapping $\Phi \colon R^M \to R^M$ with coefficients from R. One can see that $R[\xi]$ is a complete discrete valuation domain with maximal ideal $\pi R[\xi]$, and the corresponding residue field has p^{fM} elements. We thus have a notion of $\star$-cycles in $R[\xi]$, and to a $\star$-cycle in $R[\xi]$ there corresponds a $\star$-cycle in R^M.

Thus it suffices to find a $\star$-cycle in $R[\xi]$ of length $(q-1)p^n$.

Take $F(X) = \pi + \xi X + \gamma X^q + X^d$, where $d = q^2$ and $q = p^{fM}$. We remember that $\binom{0}{0} = 1$.

Lemma 1. *For any $T \geq 0$ the T-th iteration of F satisfies*

$$F^T(0) \equiv \sum_{t=1}^{T}\sum_{r=0}^{T-t} \xi^r \binom{T-t}{r} \pi^{d^{T-t-r}} + \gamma \sum_{t=1}^{T-1}\sum_{r=0}^{T-t-1} \xi^r \binom{T-t}{r} \pi^{d^{T-t-r-1}q}$$
$$\equiv \sum_{t=0}^{T-1} \xi^{-t}\pi^{d^t} A_T(t) + \gamma \sum_{t=0}^{T-2} \xi^{-(t+1)}\pi^{d^t q} A_T(t+1) \mod (p\pi, \gamma^{q+1}),$$

where $A_T(t) = \sum_{k=0}^{T-1} \binom{k}{t}\xi^k$. Moreover,

$$A_T(t) + A_T(t+1) = \xi^{-1}\big(A_T(t+1) + \xi^T \binom{T}{t+1}\big).$$

Proof. We use direct induction. One only has to remember that $\xi^q = \xi^d = \xi$ and $(x+y)^p \equiv x^p + y^p \mod (p)$. □

Lemma 2. *(i) If $q > 2$ and $T = (q-1)p^r$, then for $j = 0, 1, \dots, p^r - 1$ we have $w(A_T(j)) \geq e$, and $A_T(p^r)$ is invertible.*

(ii) If $q = 2$, then $A_T(t) = \binom{T}{t+1}$.

Proof. (i) Since $\xi \neq 1$, we have

$$A_T(0) = 1 + \xi + \dots + \xi^{T-1} = 0.$$

Using $w(\xi - 1) = 0$, simple properties of binomial coefficients and

$$A_T(t) + A_T(t+1) = \xi^{-1}\left(A_T(t+1) + \xi^T \binom{T}{t+1}\right)$$

we obtain the assertion.

(ii) In this case we have $\xi = 1$, and therefore the assertion follows from Lemma 1. □

Assume that $q > 2$. Put $\gamma = \pi^{d^{p^n-1}(d-q)} z$. In view of $(q+1)d^{p^n-1}(d-q) > d^{p^n}$ and $e \geq p^{2fNp^n} \geq d^{p^n}$ we obtain by Lemma 1 that

$$F^T(0) \equiv \sum_{t=0}^{T-1} \xi^{-t}\pi^{d^t} A_T(t) + \pi^{d^{p^n-1}(d-q)} z \sum_{t=0}^{T-2} \xi^{-(t+1)}\pi^{d^t q} A_T(t+1) \mod (\pi^{d^{p^n}+1} R[\xi, z]).$$

In particular, taking $T = (q-1)p^n$ we get, using Lemma 2,

$$F^{(q-1)p^n}(0) = \pi^{d^{p^n}} \xi^{-p^n} A_{(q-1)p^n}(p^n)\big(1 + z + \pi h(z)\big),$$

for some polynomial $h \in R[\xi][X]$. Thus $F^{(q-1)p^n}(0) = 0$ if and only if

$$1 + z + \pi h(z) = 0.$$

The existence of (a unique) $z \in R[\xi]$ satisfying $F^{(q-1)p^n}(0) = 0$ follows from the Hensel's lemma. Fix such z.

Now it is sufficient to show that the smallest $j > 0$ satisfying $F^j(0) = 0$ is $j = (q-1)p^n$.

If $F^j(0) \equiv 0 \mod (\pi^2)$, then, by Lemma 1, $A_j(0) \equiv 0 \mod (\pi)$ and $\xi^j \equiv 1 \mod (\pi)$, $q-1 \mid j$ follow. From the simple properties of cycles it follows that it suffices to show that $F^{(q-1)p^{n-1}}(0) \neq 0$. But, Lemma 1 gives

$$F^{(q-1)p^{n-1}}(0) \equiv \xi^{-p^{n-1}} A_{(q-1)p^{n-1}}(p^{n-1})\pi^{d^{p^{n-1}}} \mod (\pi^{d^{p^{n-1}}+1}),$$

and, by Lemma 2, we are done.

Assume that $q = 2$. Put $\gamma = \pi^{d^{p^n-2}(d-q)}z$. In view of $(q+1)d^{p^n-2}(d-q) > d^{p^n-1}$ and $e \geq p^{2fNp^n} \geq d^{p^n}$ we obtain by Lemma 1 that

$$F^T(0) = \sum_{t=0}^{T-1} \pi^{d^t} A_T(t) + \pi^{d^{p^n-2}(d-q)} z \sum_{t=0}^{T-2} \pi^{d^t q} A_T(t+1) \mod (\pi^{d^{p^n-1}+1}R[z]).$$

In particular, taking $T = p^n$ we get, using Lemma 2,

$$F^{p^n}(0) = \pi^{d^{p^n-1}} A_{p^n}(p^n - 1)\big(1 + z + \pi h(z)\big),$$

for some polynomial $h \in R[X]$. Thus $F^{p^n}(0) = 0$ if and only if $1 + z + \pi h(z) = 0$. The existence of $z \in R$ satisfying $F^{p^n}(0) = 0$ follows from the Hensel's lemma. Fix such z.

Now it suffices to show that the smallest $j > 0$ satisfying $F^j(0) = 0$ is $j = p^n$.

From the simple properties of cycles it follows that it suffices to show that $F^{p^{n-1}}(0) \neq 0$. But, Lemma 1 gives

$$F^{p^{n-1}}(0) \equiv A_{p^{n-1}}(p^{n-1} - 1)\pi^{d^{p^{n-1}-1}} \mod (\pi^{d^{p^{n-1}-1}+1}),$$

and, by Lemma 2, we are done.

This finishes the proof of the theorem. $\square$

Theorem 2. *(i) Let S be a Dedekind domain of characteristic $p > 0$. Let $\mathcal{F}(S)$ be the set of all natural f such that there is a nonzero prime ideal $\mathfrak{p}$ of S of norm p^f. Let $\mathcal{A}(f,N)$ consists of all numbers of the form $a \cdot b \cdot p^n$, where $a \leq p^{fN}$, $n \geq 0$ and $b \mid [p^{fa_1} - 1, \ldots, p^{fa_r} - 1]$ for some $a_1, \ldots, a_r$ satisfying $a_1 + \cdots + a_r \leq N$.*

If $N \geq 2$, then

$$\mathcal{CYCL}(S,N) = \bigcap_{f \in \mathcal{F}(S)} \mathcal{A}(f,N).$$

(ii) Let S be a discrete valuation domain of characteristic $p > 0$ such that the residue field has p^f elements. Then

$$\mathcal{CYCL}(S,1) = \{a \cdot b \cdot p^n : \ a \leq p^f,\ b \mid p^f - 1,\ n \geq 0\}.$$

Proof. Since $e = \infty$, the assertion follows from Theorem 1 and Fact 1. $\square$

Remark 1. (i) If in Theorem 2(i) $\mathcal{F}(S)$ is empty, then $\mathcal{CYCL}(S,N) = \mathbf{N}$. The similar happens to $\mathcal{CYCL}(S,1)$ in Theorem 2(ii) if $f=\infty$.

(ii) Note that $\mathcal{A}(f,N) \subseteq \mathcal{A}(fk,N)$ for any natural k. Hence, if all elements from $\mathcal{F}(S)$ are multiplicities of one element from $\mathcal{F}(S)$, then the formula in Theorem 2(i) may be significantly simplified.

Corollary 1. *We have*

$$\mathcal{CYCL}(F_p[X],2) = \{abp^n :\ a \le p^2,\ b \mid p^2-1,\ n \ge 0\}$$

and

$$\mathcal{CYCL}(F_p[X],3) = \{abp^n :\ a \le p^3,\ n \ge 0 \ \text{ and } \ b \mid p^2-1 \text{ or } p^3-1\}.$$

On the other hand

$$\mathcal{CYCL}(F_p[X],1) = \mathcal{CYCL}(F_p[X,Y],1) = \mathcal{CYCL}(F_p,1) = \{1,2,\dots,p\}.$$

Proof. Taking into account Remark 1(ii) by Theorem 2 we obtain the first part. The second part follows from $\mathcal{CYCL}(A[X],1) = \mathcal{CYCL}(A,1)$ for any domain A. □

3 A property of $\mathcal{CYCL}(R,1)$

For a domain R with unity, the set $\mathcal{A} = \mathcal{CYCL}(R) := \mathcal{CYCL}(R,1)$ satisfies

(i) $1,2 \in \mathcal{A}$;

(ii) $\mathcal{A}$ is closed under taking divisors;

(iii) for a prime p, $p \in \mathcal{A}$ implies that $\{1,2,\dots,p\} \subseteq \mathcal{A}$ (the last property follows from the Lagrange interpolation formula).

W. Narkiewicz asked in mid-nineties, whether for a subset $\mathcal{A}$ of naturals, satisfying the above properties (i), (ii), (iii), there is a domain R with $\mathcal{CYCL}(R) = \mathcal{A}$.

In this section we emphasize another property of $\mathcal{CYCL}(R)$, and thus give a negative answer to the mentioned question.

Theorem 3. *For a domain R with unity, let $\mathcal{A} = \mathcal{CYCL}(R)$. Then for a prime number p we have that $p^2 \in \mathcal{A}$ implies $\{2r : r = 1,2,\dots,p\} \subseteq \mathcal{A}$.*

Proof. Let a tuple $a_0, a_1, \dots, a_{p^2-1}$ be a cycle for $f(X) \in R[X]$. Then $0 = b_0$, $1 = b_1,\ b_2, \dots, b_{p^2-1}$, with $b_i = (a_i - a_0)/(a_1 - a_0) \in R$, is a cycle for

$$g(X) = (a_1 - a_0)^{-1}\Big(f\big((a_1-a_0)X + a_0\big) - a_0\Big) \in R[X].$$

So assume that $a_0 = 0,\ a_1 = 1$.

One proves that if $(j-i,p) = 1$, then $a_j - a_i$ is invertible. Put $d = a_p$. If $(j-i,p^2) = p$, then $a_j - a_i \sim d$. Fix $2 \le r \le p$. We are going to show that $a_0, a_1, \dots, a_{r-1}, a_p, a_{p+1}, \dots, a_{p+r-1}$ is a cycle (of length $2r$) for a suitable polynomial $f(X)$ from $R[X]$. Namely let us take as $f(X)$ the unique polynomial of degree $\leq 2r-1$ with coefficients from the field of fractions of R satisfying

$$\begin{gathered} f(a_0)=a_1\,,\quad f(a_1)=a_2\,,\quad \dots\quad ,\quad f(a_{r-1})=a_p\,,\\ f(a_p)=a_{p+1}\,,\quad \dots\quad ,\quad f(a_{p+r-1})=a_0. \end{gathered} \tag{1}$$

Put $f(X)=c_0+c_1X+\dots+c_{2r-1}X^{2r-1}$. Then (1) is equivalent to a system of linear equations with $c_0,\dots,c_{2r-1}$ to be found. From linear algebra we then get a formula for c_i.

Namely, putting $b_0=a_0,\ \dots\ ,\ b_{r-1}=a_{r-1},\ b_r=a_p,\ b_{r+1}=a_{p+1},\ \dots\ ,\ b_{2r-1}=a_{p+r-1}$, we have $c_i=\Delta_i/\Delta$, where $\Delta=\prod_{0\leq i<j\leq 2r-1}(b_j-b_i)$ and Δ_i is the determinant of the matrix

$$\begin{pmatrix} 1 & b_0 & \dots & b_0^{i-1} & b_1 & b_0^{i+1} & \dots & b_0^{2r-1}\\ 1 & b_1 & \dots & b_1^{i-1} & b_2 & b_1^{i+1} & \dots & b_1^{2r-1}\\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots\\ 1 & b_{r-1} & \dots & b_{r-1}^{i-1} & b_r & b_{r-1}^{i+1} & \dots & b_{r-1}^{2r-1}\\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots\\ 1 & b_{2r-1} & \dots & b_{2r-1}^{i-1} & b_0 & b_{2r-1}^{i+1} & \dots & b_{2r-1}^{2r-1} \end{pmatrix}.$$

We easily see that d divides all the terms in the differences of $r+1$-th and first rows, $r+2$-th and second rows,..., $2r$-th and r-th rows. Thus $d^r \mid \Delta_i$. From the properties of the differences a_j-a_i we get $\Delta\sim d^r$. Thus $c_i=\Delta_i/\Delta\in R$. □

Acknowledgements

This work is supported by the MNiSW grant N N201 366636.

References

[1] W. Narkiewicz: *Polynomial Mappings, Lecture Notes in Mathematics, vol. 1600.* Springer-Verlag, Berlin (1995).

[2] T. Pezda: Cycles of polynomial mappings in several variables over rings of integers in finite extensions of the rationals. *Acta Arith.* 108 (2) (2003) 127–146.

[3] T. Pezda: Cycles of polynomial mappings in several variables over rings of integers in finite extensions of the rationals, II. *Monatsh. Math.* 145 (2005) 321–331.

[4] J.H. Silverman: *The Arithmetic of Dynamical Systems*, Graduate Texts in Mathematics, No. 241. Springer-Verlag (2007).

[5] M. Zieve: *Cycles of Polynomial Mappings*, PhD thesis. University of California at Berkeley (1996).

Author's address:
Tadeusz Pezda: Department of Mathematics, University of Wrocław,
pl. Grunwaldzki 2/4, 50-384 Wrocław, Poland
E-mail: pezda@math.uni.wroc.pl

Received: 12 September, 2012
Accepted for publication: 31 October, 2013
Communicated by: Štefan Porubský